NetIQ® AppManager® for Cisco Unified Communications Manager Express

Management Guide

February 2012

Legal Notice

Contents

About this Book and the Library

The NetIQ AppManager product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

This guide provides information for individuals responsible for installing an AppManager module and monitoring specific applications with AppManager.

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.

User Guide for AppManager Control Center

Provides complete information about managing groups of computers, including running jobs, responding to events, creating reports, and working with Control Center. A separate guide is available for the AppManager Operator Console.

Administrator Guide for AppManager

Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.

Upgrade and Migration Guide for AppManager

Provides complete information about how to upgrade from a previous version of AppManager.

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The AppManager library is available in Adobe Acrobat (PDF) format from the NetIQ Web site: www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measureable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

1 Introducing AppManager for Cisco Unified Communications Manager Express

Cisco Unified Communications Manager Express is a unified communications solution for small business or branch offices. This solution provides call processing for Cisco IP phones as part of a converged voice and data solution empowered by a Cisco router.

AppManager is designed to help you gain easy access to Unified Communications Manager Express data, and to help you analyze and manage that data. AppManager for Cisco Unified Communications Manager Express minimizes the cost of maintaining Unified Communications Manager Express devices, aids in capacity planning, and can prevent downtime.

Cisco Unified Communications Manager Express was formerly called Cisco CallManager Express.

1.1 Features and Benefits

AppManager for Cisco Unified Communications Manager Express includes Knowledge Scripts for creating jobs that monitor the health, availability, and performance of key devices. These scripts allow you to monitor and manage crucial device properties at a depth unparalleled by any other solution. Each Knowledge Script can be configured to send an alert, collect data for reporting, and perform automated problem management when an event occurs.

With AppManager for Cisco Unified Communications Manager Express, administrators gain access to a new set of tools they can leverage to gather a wide range of diagnostic and management data, which can help prevent outages and keep things running smoothly.

The following are just a few of the features and benefits of monitoring Unified Communications Manager Express with AppManager:

- Reduces the time you spend diagnosing and resolving issues
- Monitors Unified Communication Manager Express resources, including CPU, memory, flash memory, power supplies, and temperature sensors
- Monitors the status (registered, unregistered, deceased) of phones, lets you reset IP phones and specify key phones, monitors for duplicate extensions, and takes an inventory of phones attached to Unified Communications Manager Express devices
- Monitors the IP subsystem (all packets flowing through a device) for traffic levels and percentage of packet errors
- Monitors physical interfaces for bandwidth utilization, packet loss/errors, and changes in operational status
- Monitors LAN and WAN links from a logical perspective — link utilization instead of interface utilization — for changes in operational status, bandwidth, usage, packet loss, and packet errors
- Automates system management issues that could affect device performance

- Pinpoints problems wherever they originate
- Supports Network Address Translation (NAT) on remote Unified Communication Manager Express devices

1.2 Counting AppManager Licenses

AppManager for Cisco Unified Communications Manager Express is licensed by device as part of the AppManager for Cisco CallManager module. AppManager counts the number of hardware phones registered to Unified Communications Manager Express.

2 Installing AppManager for Cisco Unified Communications Manager Express

This chapter provides installation instructions and describes system requirements for AppManager for Cisco Unified Communications Manager Express.

This chapter assumes you have AppManager installed. For more information about installing AppManager or about AppManager system requirements, see the *Installation Guide for AppManager*, which is available on the AppManager Documentation page.

2.1 System Requirements

For the latest information about supported software versions and the availability of module updates, visit the AppManager Supported Products page. Unless noted otherwise, this module supports all updates, hotfixes, and service packs for the releases listed below.

AppManager for Cisco Unified Communications Manager Express has the following system requirements:

Requirement	Version
NetIQ AppManager installed on the repository, console, and proxy agent computers	7.0 or later
Microsoft Windows operating system installed on the proxy agent computer	32-bit versions of one of the following: ◆ Windows XP Professional ◆ Windows Server 2003
Routers running Cisco Unified Communications Manager Express	3.x, 4.0, 4.1, or 4.2

If you encounter problems using this module with a later version of your application, contact NetIQ Technical Support.

2.2 Installing the Module

You can install the module in one of the following ways:

- Run the module setup program, `AM70-CiscoCME-7.x.x.0.msi`, which you downloaded from the Web or from the AppManager installation kit. Save the module setup files on the distribution computer, and then delete the older versions of the module setup files. For more information about the distribution computer, see the *Installation Guide for AppManager*
- Use Control Center to install the module on the remote computer where an agent is installed. Ensure you check in the installation package, which is the `.XML` file included with the module setup program. For more information about the `.XML` file, see the *AppManager for Cisco Unified Communications Manager Express Readme*. For more information about deploying modules on agent computers, see the *Control Center User Guide for AppManager*.

To install the module:

1. Run the module setup program on all repository computers to install the Knowledge Scripts and reports. For repositories running in a clustered environment, run the setup program on the node that currently owns the cluster resource.
2. Install the module on the proxy agent computer. Use one of the following methods:
   - Run the module setup program.
   - Use Control Center Console to deploy the installation package.
3. Run the module setup program on all Operator Console and Control Center Console computers to install the Help.
4. Configure AXL passwords and SNMP community string information in AppManager Security Manager. For more information, see Section 3.8.5, "AXL Password Configuration," on page 31 and Section 3.8.6, "SNMP Community String Configuration," on page 32.
5. If you have not already discovered Unified Communications Manager Express resources, run the Discovery_CiscoCME Knowledge Script on all proxy agent computers where you installed the module.

2.3 Silently Installing the Module

To silently (without user intervention) install a module, create an initialization file (`.ini`) for this module that includes the required property names and values to use during the installation.

To create and use an initialization file for a silent installation:

1. Create a new text file and change the filename extension from `.txt` to `.ini`.
2. To specify the community string required to access hardware resources, include the following text in the `.ini` file:

   ```
   MO_CommunityString=string name
   ```

   where *string name* is the name of the community string, such as `public`.
3. Save and close the `.ini` file.
4. Run the following command from the folder in which you saved the module installer:

   ```
   msiexec.exe /i "AM70-CiscoCME-7.x.x.0.msi" /qn MO_CONFIGOUTINI="full path to
   the initialization file"
   ```

   where *x.x* is the actual version number of the module installer.

To create a log file that describes the operations of the module installer, add the following flag to the command noted above:

```
/L* "AM70-CiscoCME-7.x.x.0.msi.log"
```

The log file is created in the folder in which you saved the module installer.

2.4 Upgrading Knowledge Script Jobs

This release of AppManager for Unified Communications Manager Express may contain updated Knowledge Scripts. You can push the changes for updated scripts to running Knowledge Script jobs in one of the following ways:

- Use the AMAdmin_UpgradeJobs Knowledge Script.
- Use the Properties Propagation feature.

2.4.1 Running AMAdmin_UpgradeJobs

The AMAdmin_UpgradeJobs Knowledge Script can push changes to running Knowledge Script jobs. Your AppManager repository (QDB) must be at version 7.0 or later. In addition, the repository computer must have hotfix 72040 installed, or the most recent AppManager Repository hotfix. To download the hotfix, see the AppManager Suite Hotfixes Web page.

Upgrading jobs to use the most recent script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job.

For more information, see the Help for the AMAdmin_UpgradeJobs Knowledge Script.

2.4.2 Propagating Knowledge Script Changes

You can propagate script changes to jobs that are running and to Knowledge Script Groups, including recommended Knowledge Script Groups and renamed Knowledge Scripts.

Before propagating script changes, verify that the script parameters are set to your specifications. Customized script parameters may have reverted to default parameters during the installation of the module. New parameters may need to be set appropriately for your environment or application.

You can choose to propagate only properties (specified in the Schedule and Values tabs), only the script (which is the logic of the Knowledge Script), or both. Unless you know specifically that changes affect only the script logic, you should propagate both properties and the script.

For more information about propagating Knowledge Script changes, see the "Running Monitoring Jobs" chapter of the *Operator Console User Guide for AppManager*.

Propagating Changes to Ad Hoc Jobs

You can propagate the properties and the logic (script) of a Knowledge Script to ad hoc jobs started by that Knowledge Script. Corresponding jobs are stopped and restarted with the Knowledge Script changes.

To propagate changes to ad hoc Knowledge Script jobs:

1. In the Knowledge Script view, select the Knowledge Script for which you want to propagate changes.

2 Click **Properties Propagation** > **Ad Hoc Jobs**.

3 Select the components of the Knowledge Script that you want to propagate to associated ad hoc jobs:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, such as schedule, monitoring values, actions, and advanced options.

Propagating Changes to Knowledge Script Groups

You can propagate the properties and logic (script) of a Knowledge Script to corresponding Knowledge Script Group members. After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. For more information, see "Propagating Changes to Ad Hoc Jobs" on page 13.

To propagate Knowledge Script changes to Knowledge Script Groups:

1 In the Knowledge Script view, select the Knowledge Script Group for which you want to propagate changes.

2 On the KS menu, select **Properties propagation** > **Ad Hoc Jobs**.

3 ***If you want to exclude a Knowledge Script member from properties propagation,*** deselect that member from the list in the Properties Propagation dialog box.

4 Select the components of the Knowledge Script that you want to propagate to associated Knowledge Script Groups:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, including the schedule, actions, and Advanced properties.

5 Click **OK**. Any monitoring jobs started by a Knowledge Script Group member are restarted with the job properties of the Knowledge Script Group member.

2.5 Monitoring for New Phones

You can use the NetworkDevice_Device_Syslog script to alert you when a new/unknown or configured/known phone registers with Unified Communications Manager Express.

A syslog message is generated whenever a new phone registers with Unified Communications Manager Express. In addition, a different syslog message is generated when an unknown phone requires Unified Communications Manager Express to create an ephone configuration entry. You can configure Device_Syslog to watch for these entries and to generate events as needed.

In the following example, a new phone registers with Unified Communications Manager Express. Unified Communications Manager Express creates an ephone entry and then forces a reset of the new phone. When the phone restarts, a normal register message is generated because the phone now

has a configuration entry. When a new phone registers and has no ephone configuration entry, the register message is IPPHONE-6-REGISTER_NEW. When a configured phone registers, the register message is IPPHONE-6-REGISTER. The following is a sample register message:

```
RalLabRT04#
19w3d: %IPPHONE-6-REG_ALARM: 25: Name=SEP000BFD07C5B3 Load=3.2(2.14)
Last=Initialized
19w3d: %IPPHONE-6-REGISTER_NEW: ephone-4:SEP000BFD07C5B3 IP:10.46.4.124 Socket:3
DeviceType:Phone has registered.  reseting 000B.FD07.C5B3
19w3d: %IPPHONE-6-UNREGISTER_NORMAL: ephone-4:SEP000BFD07C5B3 IP:10.46.4.124 Soc
ket:3 DeviceType:Phone has unregistered normally.
19w3d: %IPPHONE-6-REG_ALARM: 22: Name=SEP000BFD07C5B3 Load=3.2(2.14) Last=Reset-
Reset
```

2.6 Using NetworkDevice Knowledge Scripts

Because Cisco Unified Communications Manager Express runs on Cisco routers, the AppManager for Cisco Unified Communications Manager Express module requires the monitoring capabilities provided by Knowledge Scripts from the AppManager for Network Device module.

The AppManager for Network Device module enables you to monitor network devices such as routers, switches, and voice gateways. Using SNMP GET commands, NetworkDevice scripts monitor the basic subsystems common to all devices, such as CPU, memory, and the chassis.

Use the following NetworkDevice Knowledge Scripts to monitor the the routers. Use the CiscoCME Knowledge Scripts to monitor the phones and to perform other Unified Communications Manager Express-specific tasks, such as taking inventory, setting key phones, and resetting phones.

Knowledge Script	Description
NetworkDevice_ATMLink_Util	Monitors the usage of the parent resource of the Asynchronous Transfer Mode links on a network device.
NetworkDevice_Chassis_Usage	Monitors the physical chassis of a network device, including CPU, RAM, flash memory, backplane, temperature sensors, voltage sensors, and fan sensors.
NetworkDevice_Device_Ping	Checks the availability of network devices that respond to Internet Control Message Protocol Echo requests.
NetworkDevice_Device_Syslog	Listens for UDP traffic on port 514.
NetworkDevice_FrameRelayLink_Util	Monitors the usage of a parent resource for the frame relay links on a network device.
NetworkDevice_FXOPort_Health	Monitors signal errors on a Foreign Exchange Office port on a network device.
NetworkDevice_FXOPort_Util	Monitors Foreign Exchange Office port utilization on a network device.
NetworkDevice_FXSPort_Health	Monitors signal errors on a Foreign Exchange Station port on a network device.
NetworkDevice_FXSPort_Util	Monitors Foreign Exchange Station port utilization on a network device.
NetworkDevice_Interface_Health	Monitors the parent resource for the interfaces on a network device.
NetworkDevice_IPSubsystem_Util	Monitors the IP subsystem of a network device.
NetworkDevice_LANLink_Util	Monitors the parent resource for the LAN links on a network device.

Knowledge Script	Description
NetworkDevice_Report_ChassisUsage	Displays Good-Acceptable-Poor and average utilization for CPU, memory pool, and backplane for a network device.
NetworkDevice_Report_LinkUtilization	Displays average link utilization within a specified time frame.
NetworkDevice_Report_TotalVolume	Displays total volume for selected devices within a specified time frame.
NetworkDevice_WANLink_Util	Monitors the parent resource for the serial, T1, or T3 links on a network device.

3 CiscoCME Knowledge Scripts

Cisco Unified Communications Manager Express is a unified communications solution for small business or branch offices. This solution provides call processing for Cisco IP phones as part of a converged voice and data solution empowered by a Cisco router.

AppManager for Cisco Unified Communications Manager Express provides the following Knowledge Scripts for monitoring Cisco Unified Communications Manager Express resources. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Device_Reset	Resets Unified Communications Manager Express IP phones for reasons such as troubleshooting or picking up new default firmware.
Device_Status	Monitors the status of key Unified Communications Manager Express devices.
Extension_Check	Monitors for duplicate phone extension numbers. This script looks for all phones configured in Unified Communications Manager Express, regardless of whether they are registered.
Phone_Inventory	Generates an inventory of the phone details for phones attached to Unified Communications Manager Express.
Set_Key_Phones	Designates one or more "key" phones. After you designate key phones, you then can choose to monitor only key phones.
SRST_Failover	Monitors a device operating in SRST (Survivable Remote Site Telephony) mode for registered phones or network connectivity failure, which indicates a failover from Unified Communications Manager.
Recommended Knowledge Script Group	Performs essential monitoring of your Cisco Unified Communications Manager Express environment.
Section 3.8, “Discovery_CiscoCME,” on page 29	Discovers Cisco Unified Communications Manager Express resources, such as routers, switches, and gateways.

3.1 Device_Reset

Use this Knowledge Script to reset or restart Unified Communications Manager Express IP phones for reasons such as troubleshooting or picking up new default firmware. Use this script along with Device_Status to ensure selected phones have upgraded successfully.

NOTE

- Only an AppManager administrator should run this script.
- The AXL API does not return a failure in any of the following situations. Therefore, in each of these situations, AppManager has no way of knowing that a reset did not succeed:
  - If you try to reset an unregistered phone
  - If you try to reset a phone with an invalid or incorrect name
  - If you try to reset a phone that has never been registered with the router.

3.1.1 Resource Object

CiscoCME

3.1.2 Default Schedule

By default, this script runs once.

3.1.3 Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise event if reset/restart succeeds?	Select **Yes** to raise an event if the device was successfully reset or restarted. The default is Yes.
Event severity when reset/restart succeeds	Set the severity level of the event, from 1 to 40, to indicate the importance of a successful event. The default is 25.
Event severity when reset/restart error occurs	Set the severity level of the event, from 1 to 40, to indicate the importance of an event in which errors occurred. The default is 5.
Options	
Function type	Choose **Reset** to shut down a registered device and then bring it back up. Choose **Restart** to restart a registered device without first shutting it down. The default is Reset.

Parameter	How To Set It
Device selection type	Select the type of device you want to reset or restart. All devices of that type will be reset or restarted. ◆ Select **DeviceName** to reset or restart a specific device or devices. If you select this type, you must type a device name or list of name in the *Device name list* parameter, or identify the location of a list of devices in *Full path to file with list of devices*. ◆ Select **All** to reset or restart all phones at once. ◆ Select **AllSequenced** to reset/restart phones in sequential order. **NOTE**: The **All** and **AllSequenced** actions may take a long time to complete.
Device name list	Use this parameter if you selected **DeviceName** in the *Device selection type* parameter. Type the name of the device you want to reset or restart. You can also type a list of device names, separated by a comma. For example: `SEP999999994000,SEP999999994001`. **NOTE**: If you type a device name, ignore the *Full path to file with list of devices* parameter.
Full path to file with list of devices	Use this parameter if you selected **DeviceName** in the *Device selection type* parameter. Type the full path to a file on the agent computer containing a list of the devices you want to restart or reset. The file should contain the device names on one or more lines. If you specify the criteria on one line, separate each item with a comma. For example: `SEP999999994000,SEP999999994001`. If you specify the criteria on multiple lines, ensure each line contains only one entry. For example: ◆ SEP999999994002 ◆ SEP999999994000 ◆ SEP999999994004 **NOTE**: If you type a file path, ignore the *Device name list* parameter.

3.2 Device_Status

Use this Knowledge Script to monitor the status of key Unified Communication Manager Express devices. The possible statuses are:

- **Registered**. This status indicates the device is available.

- **Unregistered**. This status indicates a device previously registered with Unified Communication Manager Express has become unregistered. This status may be generated as part of a normal unregistration event, or can be due to another reason such as loss of keepalives.
- **Deceased**. This status indicates the device has not been registered to Unified Communication Manager Express for a long time, or the device was added to Unified Communication Manager Express but never registered.

NOTE: Phones of model type 7905G are designated in event messages as an "Others" type. (Cisco issue `CSCee28952`)

The first time you run this script, it builds a device list from the criteria you have selected. At each subsequent interval, the script checks the status of these devices. If the number or percentage of these devices that are registered does not meet the threshold you set, an event is raised.

3.2.1 Resource Object

CiscoCME

3.2.2 Default Schedule

By default, this script runs every one minute.

3.2.3 Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise event if key devices fall below threshold?	Select **Yes** to raise an event if the number or percentage of registered key devices falls below the threshold you set. The default is Yes. The detailed message for an event contains the following information about each device that is not registered: ◆ Device Name ◆ Directory numbers ◆ IP address (if available) ◆ Status ◆ Unified Communication Manager Express address where device was registered (if available) ◆ Model
Event severity when key devices fall below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number or percentage of key devices fell below the threshold. The default is 10.

Parameter	How To Set It
Raise event if key devices cross threshold and then return?	Select **Yes** to raise an event if the number or percentage of key devices falls below the minimum, but is now within an acceptable range. The default is Yes. The detailed message for the event will contain the percentage of registered devices and the threshold percentage.
Event severity when key devices cross threshold and then return	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number or percentage of key devices fell below the minimum, but is now within an acceptable range. The default is 20.
Raise initial event with current status?	Select **Yes** to raise an informational event that contains the current status of selected devices. The default is Yes. This event is raised only upon the first run of this script. The event message returns the following details about each device: ◆ Device Name ◆ Directory numbers ◆ IP address (if available) ◆ Status ◆ Unified Communication Manager Express address where device was registered (if available) ◆ Model
Format status event in XML?	Select **Yes** to format the informational event containing the current status in XML. The default is Yes. If you use XML for the event, it will not be sent to any Actions defined for the script. If you want this information sent to an Action, do not select this checkbox. The detailed message will then be formatted in .csv format.
Event severity for initial event with current status	Set the severity level, from 1 to 40, to indicate the importance of the informational event. The default is 30.
Data Collection	
Collect data?	Select **Yes** to collect data for graphs and charts. If enabled, data collection returns the number of devices being monitored and the number of those devices that are registered. The default is unchecked.
Monitoring	
Select by type	Choose the type of the selection criteria to be used to get the list of devices to monitor. Some criteria may not make sense for every device type. Valid values are: ◆ DeviceName, which is the default ◆ KeyPhones

Parameter	How To Set It
Selection criteria	Specify the selection criteria for the devices to be monitored. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all devices with device names that begin with SEP, type `SEP*`. The wildcard works only at the end of a string. To monitor all devices, accept the default of *. You can type multiple items by separating each item with a comma. For example: `SEP0009A*,SEP0009B*` . **NOTE**: If you type a file path in *Full path to file with list of selection criteria,* ignore this parameter.
Full path to file with selection criteria	Specify the full path to a file on the agent computer containing a list of the selection criteria. The file should contain the selection criteria on one or more lines. You can specify the actual item or you can specify a pattern by using the * wildcard. If you specify the criteria on one line, separate each item with a comma. For example: `SEP0009A*,SEP0009B*`. If you specify the criteria on multiple lines, ensure each line contains only one entry. For example: ◆ SEP0009A* ◆ SEP999999994000 ◆ SEP00044* **NOTE**: If you type a file path, ignore the *Selection criteria* parameter.
Threshold type	Select whether you want to monitor for a **Percentage** threshold or a **Number** threshold. The default is percentage.
Threshold - Minimum % devices registered	Specify the minimum percentage of devices that must have a status of "Registered" before an event is raised. The default is 75%.
Threshold - Minimum # devices registered	Specify the minimum number of devices that must have a status of "Registered" before an event is raised. The default is 0.

3.3 Extension_Check

Use this Knowledge Script to monitor for duplicate phone extension numbers. This script will look for all phones configured in Unified Communications Manager Express, regardless of whether they are registered. This script automatically raises an event if duplicate extension numbers are discovered.

3.3.1 Resource Object

CiscoCME

3.3.2 Default Schedule

By default, this script runs every four hours.

3.3.3 Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise event if no duplicate extensions found?	Select **Yes** to create an event if no duplicate extension numbers are discovered. The default is Yes.
Event severity when no duplicate extensions found	Set the severity level, from 1 to 40, to indicate the importance of an event in which no duplicates are found. The default is 25.
Event severity when duplicate extensions found	Set the severity level, from 1 to 40, to indicate the importance of an event in which duplicates are found. The default is 10.

3.4 Phone_Inventory

Use this Knowledge Script to create an inventory of phone details for phones attached to Unified Communications Manager Express.

NOTE: Phones of model type 7905G are designated in event messages as an "Others" type. (Cisco issue `CSCee28952`)

3.4.1 Resource Object

CiscoCME

3.4.2 Default Schedule

By default, this script runs once.

3.4.3 Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise informational event when inventory completes?	Select **Yes** to raise an event when the inventory is complete. The event message contains the phone inventory details. The default is Yes.
Event severity when informational event is raised	Set the severity level of the event, from 1 to 40, to indicate the importance an informational event. The default is 25.
Event severity when no phones are found	Set the severity level of the event, from 1 to 40, to indicate the importance of an event in which no phones are found. The default is 30.
Event severity when inventory fails	Set the severity level of the event, from 1 to 40, to indicate the importance of an event in which the inventory fails. The default is 15.

Parameter	How To Set It
Selection Options	
Select by	Choose the type of the selection criteria you want to use to create the list of phones. Valid values are: ◆ Name, which is the default ◆ KeyPhones
Selection criteria	Specify the selection criteria for the devices to be monitored. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all devices with device names that begin with SEP, type `SEP*`. The wildcard works only at the end of a string. To monitor all devices, accept the default of `*`. You can type multiple items by separating each item with a comma. For example: `SEP0009A*,SEP0009B*`. **NOTE**: If you type selection criteria, then ignore the *Full path to file with selection criteria* parameter.
Full path to file with selection criteria	Specify the full path to a file on the agent computer containing a list of the selection criteria. The file should contain the selection criteria on one or more lines. You can specify the actual item or you can specify a pattern by using the * wildcard. If you specify the criteria on one line, separate each item with a comma. For example: `SEP0009A*,SEP0009B*`. If you specify the criteria on multiple lines, ensure each line contains only one entry. For example: ◆ SEP0009A* ◆ SEP999999994000 ◆ SEP00044* **NOTE**: If you type a file path, ignore the *Selection criteria* parameter.
Result File Options	
Write details to result file?	Select **Yes** to output the inventory results to a .csv file. The default is Yes.

Parameter	How To Set It
Result file name	Specify the full path or a UNC path to a location on the agent computer where the inventory result file should be written. The default location is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventory`. The following details are returned about each phone: ◆ Name ◆ Directory numbers ◆ Model ◆ IP address (if available) ◆ Unified Communications Manager Express where device is\was registered (if available) ◆ Status ◆ Status Time **NOTE**: The Phone_Inventory script can be run against multiple devices at one time. To avoid confusion, the name of the device is added to the name of the output file. The inventory results for each device are output to a separate file, identified by the device name.
Overwrite existing file?	Select **Yes** to overwrite the existing file. Disable this parameter to add any new results to the existing file. The default is unselected. **Warning** Deselecting Yes and then running the script many times could result in the creation of a very large file.
List only phone with status of	Use this parameter to limit the phones listed in the results file to only those whose status is one of the following: ◆ Any, which is the default ◆ Not Registered ◆ Registered ◆ Unregistered ◆ Deceased **NOTE**: Setting this parameter to a value of **Not Registered** will list those phones with a status of Unregistered or Deceased.
Order by	Accept the default of **Name** to display the contents of the results file in order by the phone name. Select **DirectoryNumber** to display the contents of the results file in order by directory number.

3.5 Set_Key_Phones

Use this Knowledge Script to designate one or more phones as “key” phones. The “key phone” feature of Unified Communications Manager Express allows you to specify certain phones to be used for monitoring or management purposes. For example, you may not want to monitor all phones at a particular location, but instead monitor only a select subset of important, or key, phones.

The AXL API identifies which phones are key and which are not.

NOTE

- This script does not support devices operating in SRST (Survivable Remote Site Telephony) mode. Devices go into SRST mode when the WAN link to the Cisco Unified Communications Manager at the central site goes down, or when the connection to the Unified Communications Manager is lost.
- You cannot designate an ATA186 device as a key phone. (Cisco issue `CSCee28929`)

3.5.1 Removing Key Phones

The "key phone" feature of Unified Communications Manager Express allows you to specify certain key phones to be used for monitoring or management purposes. For example, you may not want to monitor all phones at a particular location, but instead monitor only a select subset of important phones.

Although you can use a Knowledge Script to set a key phone, you need to use the IOS configuration command line interface to remove a key designation from a phone. The following is an example of removing a key designation from a phone using Ethernet phone (ephone) entry number 4.

```
RalLabRT04#config t
RalLabRT04(config)#ephone 4
RalLabRT04(config-ephone)#no keyphone
RalLabRT04(config-ephone)#exit
RalLabRT04(config)#exit
```

3.5.2 Resource Object

CiscoCME

3.5.3 Default Schedule

By default, this script runs once.

3.5.4 Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise event if key designation succeeds?	Select **Yes** to generate an event when key phones are successfully designated. The default is Yes.
Event severity when key designation succeeds	Set the severity level of the event, from 1 to 40, to indicate the importance of an event in which key phones are successfully designated. The default is 25.
Event severity when key designation fails	Set the severity level of the event, from 1 to 40, to indicate the importance of the event in which the key designation attempt fails. The default is 5.
Set Options	

Parameter	How To Set It
List of phones	Specify the names of phones you want to designate as key phones. You must specify at least one phone. You can type multiple names by separating them with a comma. For example: `SEP999999994002,SEP999999994007`. **NOTE**: If you type a list of phones, ignore the *Full path to file with list of phones* parameter.
Full path to file with list of phones	Specify the full path to a file on the agent computer containing a list of the names of key phones. The file should contain the names on one or more lines. If you specify the key phones on one line, separate each item with a comma. For example: `SEP999999994000,SEP999999994001`. If you specify the phones on multiple lines, ensure each line contains only one entry. For example: ◆ SEP999999994002 ◆ SEP999999994000 ◆ SEP999999994004 **NOTE**: If you type a full path, ignore the *List of phones* parameter.

3.6 SRST_Failover

Use this Knowledge Script to monitor for registered phones or connectivity failure to the SRST (Survivable Remote Site Telephony) device, which indicate a failover has occurred. A device operating in SRST mode can be monitored for SRST failover. Failover occurs when the WAN link to the Unified Communications Manager at the central site goes down, or when the connection to the Unified Communications Manager is lost.

During SRST failover, there may be no connectivity at all to the remote site and the SRST router. With no connectivity, AppManager cannot access the SRST router to determine whether phones are registered. Therefore, you can choose to have this script script raise an event when connectivity has failed.

All CiscoCME Knowledge Scripts work with SRST mode except Set_Key_Phones. Because SRST mode does not provide any phone configuration information, you cannot set an SRST phone to be a key phone.

This script raises events that identify registered phones and connectivity failures.

NOTE: This script cannot be used on a router operating in CME mode.

3.6.1 Resource Object

CiscoCME

3.6.2 Default Schedule

By default, this script runs once.

3.6.3 Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise event when phones register with SRST?	Select **Yes** to raise an event when phones register with SRST, indicating failover. The default is Yes.
Event severity when phones register with SRST	Set the severity level, from 1 to 40, to indicate the importance of an event in which phones register with SRST. The default is 10.
Raise event when connectivity fails?	Select **Yes** to raise an event when connectivity failure occurs. The default is Yes.
Event severity when connectivity fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which connectivity fails. The default is 10.

3.7 Recommended Knowledge Script Group

The following Knowledge Scripts are members of the CiscoCME Knowledge Script Group. You can find these scripts individually on the CiscoCME tab and in a group on the RECOMMENDED tab of the Operator Console.

- Device_Status
- Extension_Check

All scripts in the KSG have their parameters set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the CiscoCME group on a Unified Communications Manager Express resource.

The CiscoCME KSG enables a “best practices” usage of AppManager for monitoring your Cisco Unified Communications Manager Express environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView.

A KSG is composed of a subset of a module’s Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the CiscoCME tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoCME tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the CiscoCME KSG and want to restore it to its original form, you can reinstall AppManager for Cisco Unified Communications Manager Express on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\CiscoCME` directory.

3.8 Discovery_CiscoCME

Use this Knowledge Script to discover Cisco Unified Communications Manager Express resource and configuration information.

3.8.1 Prerequisite

Configure the AXL password and the SNMP community string in AppManager Security Manager.

3.8.2 Resource Object

You should only have one computer acting as proxy for any given Communications Manager Express device. Therefore, run this script on only one computer at a time.

3.8.3 Default Schedule

By default, this script runs once for each server.

3.8.4 Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Auto Discovery	
Default gateway router	Specify the IP network address of the gateway (router) to query during discovery. **NOTE**: Use this parameter if you are not certain of all the relevant subnets that should be scanned during discovery. If you type an IP address here, AppManager queries the gateway for its routing tables and then attempts to discover every device in the tables.
Maximum number of hops	Specify the maximum number of hops you want discovery to make during auto-discovery. The default is one hop. Discovery considers the gateway router itself to be the first hop. Therefore, a *Maximum number of hops* setting of 1 means you will discover only the networks directly connected to the gateway router, but no other routers. To discover more, type a *Maximum number of hops* setting of at least 2.
List of devices	Use this parameter if you know which Unified Communications Manager Express devices you want to discover. Type a list of the devices you want to discover. You must specify at least one device. Use a comma to separate the names in the list: `raldbellijm02,raldattixlm` You can type hostnames (if you use DNS in your environment) or IP addresses.

Description	How To Set It
List of device ranges	Specify a list of IP address ranges for the Unified Communications Manager Express devices you want to discover. Spaces are invalid in the list; only numbers, dashes, periods, and commas are allowed. For example: `10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254` **NOTE**: Limit the number of IP addresses in each range to no more than 256. To scan more than 256 IP addresses, break a range into multiple ranges, each with no more than 256 IP addresses.
Full path to file with list of devices	Instead of listing each device separately, you can specify the full path to a file on the proxy computer that contains host names or IP addresses. The file should contain the names on one or more lines. If you specify the devices on one line, separate each item with a comma. For example: `10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254` If you specify the devices on multiple lines, ensure each line contains only one entry. For example: ◆ SEP999999994002 ◆ SEP999999994000 ◆ SEP999999994004
Discovery Details	To improve console performance, set the *Discover individual ...* parameters to **No** for any device you do not want to monitor. By not displaying these objects in the TreeView pane, you will significantly speed discovery and improve the performance of the TreeView pane of the Operator Console.
Discover individual interfaces?	Set to **y** to discover individual interfaces. The default is y.
Discover individual LAN links?	Set to **y** to discover individual LAN links. The default is y.
Discover individual WAN links?	Set to **y** to discover individual WAN links. The default is y.
Discover individual frame relay links?	Set to **y** to discover individual frame relay links. The default is y.
Discover individual ATM links?	Set to **y** to discover individual ATM links. The default is y.
Discover individual FXS ports?	Set to **y** to discover individual FXS ports. The default is y.
Discover individual FXO ports?	Set to **y** to discover individual FXO ports. The default is y.
Discover individual ISDN channels?	Set to **y** to discover individual ISDN channels. The default is y.
Discovery timeout	Specify the number of minutes the script should attempt discovery before stopping as unsuccessful. The maximum is 60. The default is 10 minutes.
Raise event if discovery succeeds?	This script always raises an event when discovery fails for any reason. In addition, you can set this parameter to **y** to raise an event when discovery succeeds. The default is n.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.

3.8.5 AXL Password Configuration

AVVID XML Layer (AXL), a Cisco application programming interface (API), enables Unified Communications Manager Express to access the HTTP server.

Most of the AXL information is configured in an IOS configuration mode called telephony-service. In order for the CiscoCME Knowledge Scripts to function properly, you should review and then take action on the following:

- `xmltest` cannot be configured on the Unified Communications Manager Express router. This configuration keyword puts the AXL (AVVID XML Layer) into interactive test mode. If `xmltest` is configured, the AXL queries the CiscoCME Knowledge Scripts use will not work. Use the following IOS command to disable `xmltest`:

  ```
  config t, telephony-service, no xmltest
  ```

- Configure an AXL password using the log password IOS command. Then configure this password into AppManager Security Manager. If you do not specifically configure an AXL password, configure the Router Privilege Mode password in Security Manager to authorize AXL requests.
- If the `xmlschema` keyword is configured on the Unified Communications Manager Express router, the CiscoCME Knowledge Scripts may not work properly. This configuration keyword specifies the location of the XML schema for AXL. By default, the Knowledge Scripts use the default schema location. If you change the keyword to something other than the default, the Knowledge Scripts will not be able to identify the schema location.

If your AXL password information is the same for all Unified Communications Manager Express devices, complete the following procedure once. If your AXL password information is different for different devices, complete the following procedure once for each different password.

If, after running Section 3.8, "Discovery_CiscoCME," on page 29, you do not see the expected devices in the TreeView pane of the Operator Console, ensure you configured the correct AXL password. To do so, perform the following procedure again.

On the Custom tab in Security Manager, complete the following fields.

Field	Description
Label	`CiscoCME`
Sub-label	Indicates whether the AXL password applies to one router or all routers. ◆ For a single router, type the device name. ◆ For all routers, type `default`.
Value 1	AXL password you configured using the "og password" IOS command on the router. If you did not configure an AXL password, type the "Router privilege mode" password
Extended application support	Encrypts the AXL password in Security Manager. Do not leave this option unselected.

3.8.6 SNMP Community String Configuration

To enable SNMP access of Unified Communications Manager Express devices, configure the SNMP read-only community strings in AppManager Security Manager.

If your community string information is the same for all Unified Communications Manager Express devices, complete the following procedure once. If your community string information is different for different devices, complete the following procedure once for each different community string.

On the Custom tab in Security Manager, complete the following fields.

Field	Description
Label	`NetworkDevice`
Sub-label	Indicates whether the AXL password applies to one router or all routers. ◆ For a single router, type the router IP address. ◆ For all routers, type `default`.
Value 1	Appropriate read-only community string, such as `private` or `public`.